CLAIMS

1. A security device comprising two or more magnetic elements, wherein said magnetic elements are responsive to switch magnetisation state in response to an applied magnetic field to provide a characteristic response, characterised in that the elements are made of magnetically soft material that discretely switches magnetisation state at an applied field strength that depends upon inherent structural variations that are present in the magnetically soft material.

2. The security device of Claim 1, wherein the security device stores a premeasured characteristic response.

3. The security device of Claim 1 or Claim 2, wherein said characteristic response represents an aggregate response of said magnetic elements to said applied magnetic field.

4. The security device of any preceding Claim, wherein said magnetic elements are supported by a substrate.

5. The security device of Claim 4, wherein said magnetic elements are supported on said substrate.

6. The security device of any preceding Claim, wherein the magnetic elements comprise thin layer magnetic material.

7. The security device of Claim 6, wherein the thin layers of magnetic material are less than 1 μm thick.

8. The security device of Claim 7, wherein the thin layers of magnetic material between 10 nm and 100 nm thick.

9. The security device of any preceding Claim, wherein said magnetic elements are responsive to said applied magnetic field to switch the magnetisation or magnetic polarisation of at least one of the magnetic elements.

10. The security device of any preceding claim, wherein at least one of the magnetic elements comprises a magnetically soft material selected from one or more of: nickel, iron, cobalt and alloys thereof with each other or silicon, such as nickel iron alloy, cobalt iron alloy, iron silicon alloy or cobalt silicon alloy.

11. The security device of Claim 10, wherein said magnetically soft material is a permalloy material.

12. The security device of any preceding Claim, wherein at least one of the magnetic elements is substantially wire-shaped or flattened wire shaped.

13. The security device of any preceding Claim, wherein the device comprises a generally parallel array of elongate rectangular magnetic elements.

14. The security device of Claim 13, wherein the magnetic elements comprise an array of generally parallel magnetic nanowires.

15. The security device of any preceding Claim, wherein the magnetic elements have generally the same size and/or shape.

16. The security device of any preceding Claim, wherein several discrete groups of differently sized and/or shaped magnetic elements, the magnetic elements being generally similarly sized and/or shaped within each group, are provided so that several different switching fields can be identified.

17. The security device of Claim 16, comprising an ensemble of rectangular magnetic elements in parallel array including several discrete groups of magnetic elements of different widths.

18. The security device of any preceding Claim, wherein differently sized and/or shaped magnetic elements are provided in a continuously varying array, so that variations in sized and/or shape between a magnetic element and its neighbours are minimised to avoid large discontinuities.

19. The security device of Claim 18, comprising an ensemble of rectangular magnetic elements in parallel array of width varying continuously across the array.

20. The security device of any preceding Claim, further comprising a single relatively large area magnetic element for use as a reference element.

21. The security device of any preceding Claim, wherein at least one of the magnetic elements is backed by a light reflective layer.

22. The security device of any preceding Claim, wherein at least one of the magnetic elements is provided proximal a reduced light reflectivity portion of said security device.

23. The security device of any preceding Claim, wherein the magnetic elements are arranged to provide a linear pattern.

24. The security device of any preceding Claim, wherein said magnetic elements are arranged to provide a two-dimensional pattern.

25. The security device of any preceding Claim, further comprising a unique identifier incorporated therewith.

26. The security device of claim 25, wherein said unique identifier is provided by way of one or more of: an optically readable bar code; one or more optical indicia; a magnetically encoded identifier; and an electronic identifier.

27. The security device of claim 26, mounted upon a smart-card, wherein said electronic identifier is provided by a smart-card chip provided on said smart-card.

28. The security device of any preceding Claim, wherein premeasured characteristic response information representing one or more measurable parameters of said characteristic response is stored on said security device.

29. The security device of Claim 28, wherein said premeasured characteristic response information is in encrypted form.

30. The security device of Claim 29, wherein said premeasured characteristic response information is encrypted using an asymmetric encryption algorithm with the private key used for enciphering being kept secret and the public key used for deciphering being made available to any reader of the security device.

31. The security device of Claim 2 or any one of Claims 3 to 30 when dependent on Claim 2, wherein the premeasured characteristic response is stored in machine-readable form.

32. A method of manufacturing a security device, comprising:

providing two or more magnetic elements made of magnetically soft material having random variations introduced into the magnetically soft material during fabrication, wherein said magnetic elements discretely switch magnetisation state in response to an applied magnetic field in order to generate a characteristic response.

33. The method of Claim 32, comprising providing said magnetic elements on a substrate.

34. The method of Claim 32 or Claim 33, comprising forming at least one of the magnetic elements using a lift off or wet etching process.

35. The method of Claim 32 or Claim 33, comprising forming at least one of the magnetic elements using an ion beam etching process.

36. The method of any one of Claims 32 to 35, comprising measuring the magnitude(s) of one or more magnetic parameters of said magnetic elements.

37. The method of Claim 36, comprising measuring one or more of coercivity and jitter values.

38. The method of Claim 36 or Claim 37, comprising using the measured magnitude(s) of said one or more magnetic parameters to represent premeasured characteristic response information.

39. The method of Claim 38, comprising encrypting said premeasured characteristic response information.

40. The method of Claim 38 or Claim 39, comprising storing said premeasured characteristic response information in encrypted or unencrypted form on said security device.

41. The method of Claim 38 or Claim 39, comprising storing said premeasured characteristic response information in encrypted or unencrypted form in a storage medium remote from said security device.

42. The method of Claim 41, comprising storing said premeasured characteristic response information in encrypted or unencrypted form in a database.

43. The method of any one of Claims 32 to 42, further comprising providing said security device with a unique identifier.

44. The method of Claim 43 when dependant upon any one of Claims 38 to 42, comprising storing a representation of said unique identifier in association with said premeasured characteristic response information.

45. A system for reading a security device, comprising:

a magnetic field generation system for applying a magnetic field to the security device according to any one of claims 1 to 31 comprising two or more magnetic elements; and

a detection system for measuring one or more discrete magnetisation switching parameters representative of a measured characteristic response of said security device generated in response to said magnetic field,

wherein said system is operable to compare said one or more discrete magnetisation switching parameters representative of a measured characteristic response to one or more respective parameters of a premeasured characteristic response to determine whether respective measured and premeasured parameters are substantially equivalent.

46. The system of Claim 45, wherein said measured characteristic response and said premeasured characteristic response are representative of an aggregate response produced by said two or more magnetic elements.

47. The system of Claim 45 or Claim 46, wherein the magnetic field generation system is operable to apply a time varying magnetic field to a security device.

48. The system of any one of Claims 45 to 47, wherein a light beam is used to interrogate said security device.

49. The system of Claim 48, wherein said light beam is a visible or near-infrared beam produced by a laser diode.

50. The system of any one of Claims 45 to 49, wherein said parameters represent one or more of coercivity and jitter values.

51. The system of any one of Claims 48 to 50, wherein said detection system incorporates magneto-optic Kerr effect detection apparatus for detecting changes induced in said light beam by magnetic elements of said security device.

52. The system of Claim 51, wherein said magneto-optic Kerr effect detection apparatus is configured to operate in transverse mode.

53. The system of any one of Claims 45 to 52, further operable to deflect said light beam across the surface of said security device.

54. The system of any one of Claims 45 to 53, further operable to read a unique identifier from said security device.

55. The system of Claim 54, wherein said unique identifier is identified by reading one or more of: an optically readable bar code; one or more optical indicia; a magnetically encoded identifier; and an electronic identifier.

56. The system of any one of Claims 45 to 55, further operable to determine said one or more respective parameters of the premeasured characteristic response by reading said one or more parameters from said security device.

57. The system of any one of Claims 45 to 56, further operable to determine said one or more respective parameters of the premeasured characteristic response by reading said one or more parameters from a database.

58. The system of Claim 57, wherein said database is remotely located from said detection system.

59. The system of any one of Claims 45 to 58, further operable to decrypt premeasured characteristic response information where it is read or provided in encrypted form.

60. A method for reading the security device according to any one of claims 1 to 31, comprising:

applying a magnetic field to a security device comprising two or more magnetic elements made of magnetically soft material;

measuring one or more discrete magnetisation switching parameters representative of a measured characteristic response of said security device generated in response to said magnetic field; and

comparing said one or more discrete magnetisation switching parameters representative of a measured characteristic response to one or more respective parameter(s) of a premeasured characteristic response to determine whether respective measured and premeasured parameters are substantially equivalent.

61. The system of Claim 60, wherein said measured characteristic response and said premeasured characteristic response are representative of an aggregate response produced by said two or more magnetic elements.

62. The method of Claim 60 or Claim 61, comprising applying a time varying magnetic field to a security device.

63. The method of any one of Claims 60 to 62, wherein measuring of one or more parameters representative of a measured characteristic response of said security device generated in response to said magnetic field comprises measuring one or more of coercivity and jitter values.

64. The method of any one of Claims 60 to 63, comprising interrogating said security device using a light beam.

65. The method of any one of Claims 60 to 64, comprising operating a laser to produce a visible or near-infrared beam.

66. The method of Claim 64 or Claim 65, comprising detecting changes induced in said light beam by magnetic elements of said security device using the magneto-optic Kerr effect.

67. The method of Claim 66, comprising using the magneto-optic Kerr effect transverse mode.

68. The method of any one of Claims 60 to 67, comprising reading a unique identifier from said security device.

69. The method of Claim 68, comprising identifying said unique identifier by reading one or more of: an optically readable bar code; one or more optical indicia; a magnetically encoded identifier; and an electronic identifier.

70. The method of any one of Claims 60 to 69, comprising determining said respective one or more parameters of the premeasured characteristic response by reading said one or more parameters from said security device.

71. The method of any one of Claims 60 to 70, comprising determining said one or more respective parameters of the premeasured characteristic response by reading said one or more parameters from a database.

72. The method of Claim 71, comprising accessing a database remotely located from said detection system.

73. The method of any one of Claims 60 to 72, further comprising decrypting premeasured characteristic response information where it is read or provided in encrypted form.

74. A product comprising the security device of any one of Claims 1 to 31.

75. The product of Claim 74, comprising one or more of: a document; a passport; an identity card; a compact disc; a digital versatile disc; a software product; packaging; an item of clothing; an item of footwear; a smart-card; a credit or bank card; a cosmetic item; an engineering part; an accessory; and any other goods and/or items of commerce, whether manufactured or otherwise.